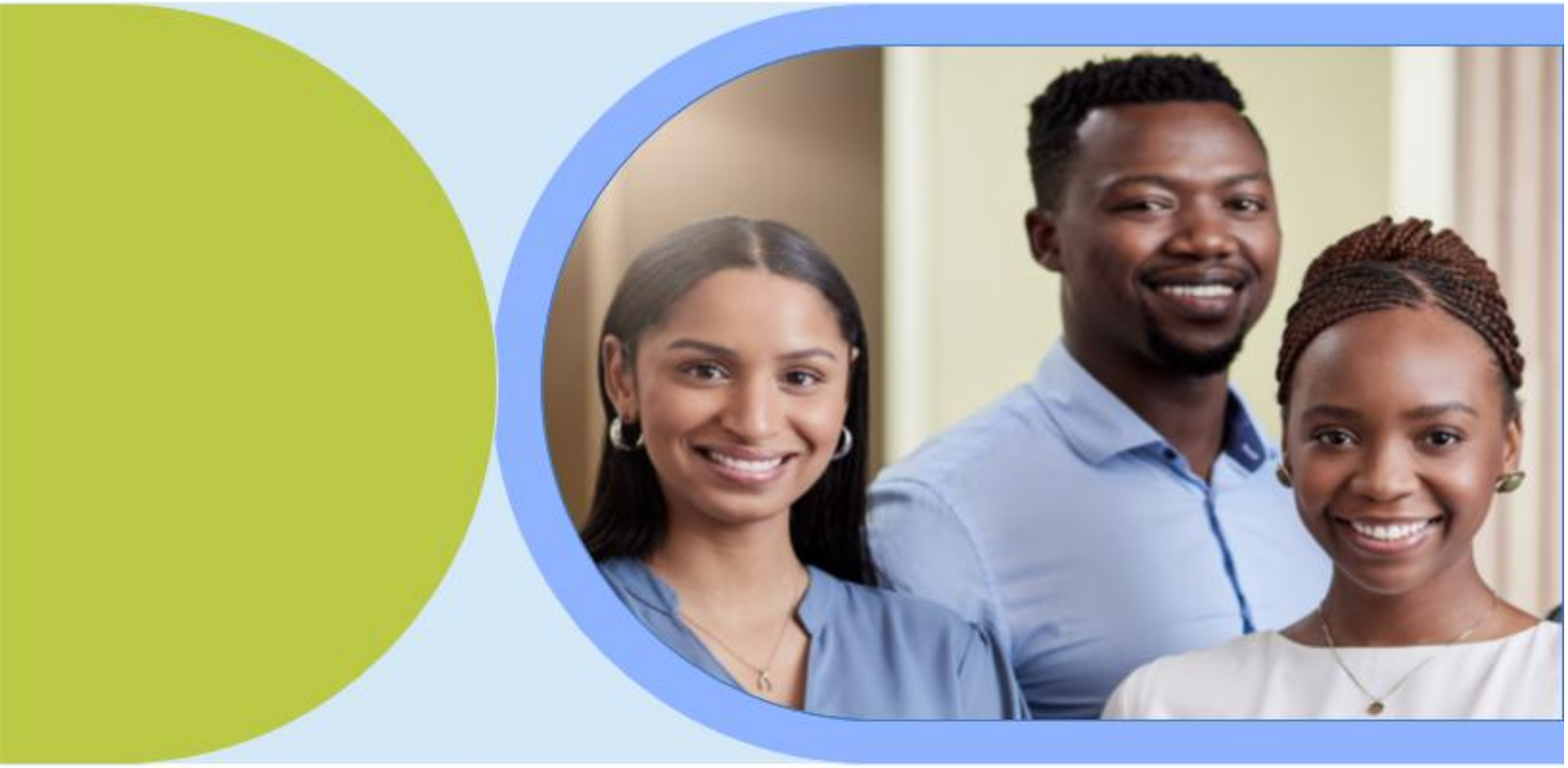
Crown Commercial Service

zensar



Zensar's Service Definition Document for Security Operations Centre (SOC)

January 2026

Disclaimer & Confidentiality

The information in this document shall not be disclosed outside the Crown Commercial Service and shall not be duplicated, used or disclosed, in whole or in part, for any purpose other than to evaluate the document. This restriction does not limit the right of the Crown Commercial Service to use information contained in this document if it is obtained from another source without restriction. This proposal is valid up to 90 days from the date of submission of the proposal.

Table of Contents

1 Introduction

The purpose of this document is to describe the ZenSOC Service description document; Service Setup, SLA, Components and Operation so that it may be used as a reference point by client to understand ZenSOC.`

In today's world of ever more complex, widely distributed and difficult to manage networks the role of Security Information and Event Management (SIEM) is increasingly important. Be it to comply with government regulations and compliance standards or to protect personal data and be seen to be doing so; having a Prescriptive SOC is now a vital part of protecting not only your data but also, your brand.

Virtually every regulatory mandate requires some form of log management to maintain an audit trail. SIEMs provide a mechanism to rapidly and easily deploy a log collection infrastructure that directly supports this requirement and allows both access to recent log data, as well as archival and retrieval of older log data.

This document gives you a detailed overview of Microsoft Sentinel such as high-level architecture, integration with Microsoft products and third-party products such as Defender for endpoint, Defender for Cloud, Defender for Identity, Defender for O365, Windows, Linux, firewalls, AWS Guard Duty, ITSM etc. Also, it will guide you to deploy Microsoft Sentinel step-by-step which includes initial configuration, data sources integration, enabling analytics rules, creating custom rules, enabling fusion rules, creating playbooks and a high level understanding of KQL query.

ZenSOC is a 24/7 Managed cyber threat protection & remediation service, monitoring your infrastructure, systems, network and applications for security events with integrated assistance from the latest threat intelligence feeds.

We take complete end-to-end ownership of our service delivery, these capabilities are delivered through a global network of SOC's providing service to you 24x7x365.

ZenSOC reports on activity outside the normal indicating a potential security threat e.g. malware. This allows analysts to quickly spot suspicious behaviour & cyber-attacks and take action to prevent them. The primary objective of Cloud SIEM is actionable Intelligence and to remain safe in breach. Our ZenSOC will detect and respond to changing cyber-attacks of all types; where the mitigation of this attack requires customer action supporting data to enable the customer to decide upon the control action required. Of course, if Zensar manages a security component on the customers' behalf we will take the required mitigation action and notify the customer we have done this. For customers where Zensar manages multiple customer security components our actionable Intelligence approach can become a Detection and Response service across the Security Infrastructure.

ZenSOC is powered by Microsoft Sentinel, rated as the industry leader. This is delivered on a fully managed service model; combining scalability with a resilient and secure Cloud hosted service. This approach provides a usage based Threat Monitoring and hunting Service that customers can pay for on an Op-ex basis.

Customers will have access to a ZenSOC MDR dashboard that, provides visibility in real-time of Security Events and anomalous activity that have been detected in the customer environment.

ZenSOC will also provide a number of security reports summarising security event information on a daily, weekly and monthly basis.

2 Architecture and Components

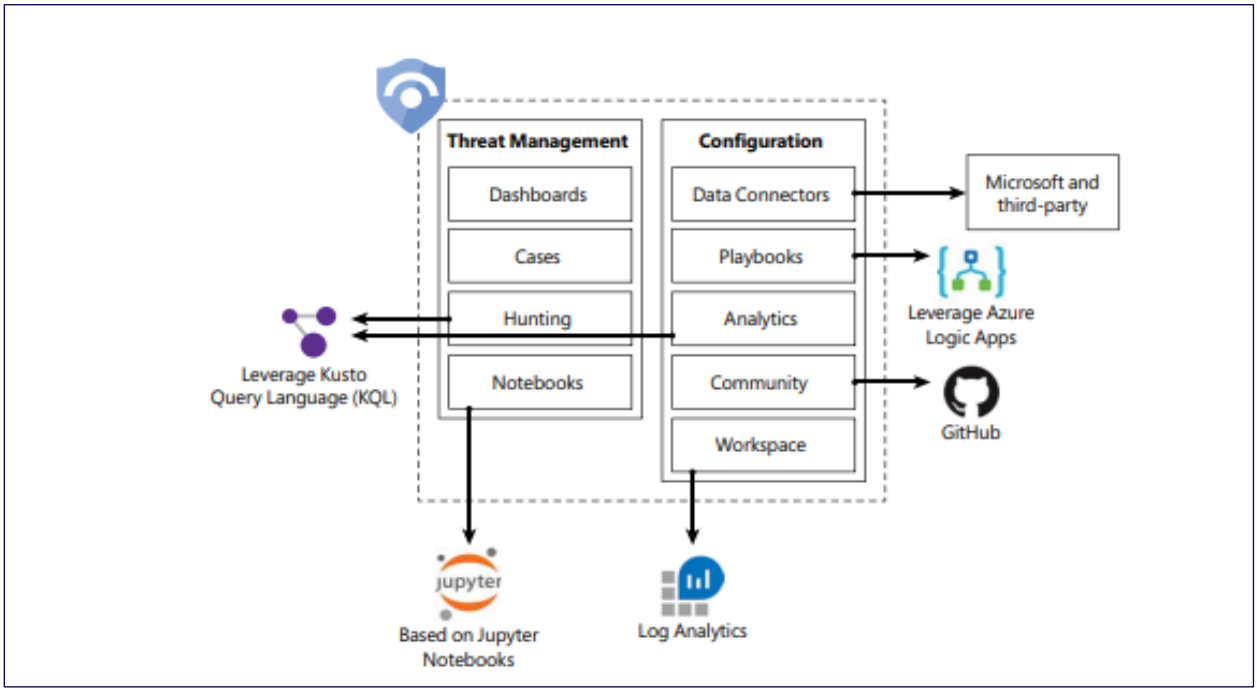
ZenSOC MDR s a fully managed Security Threat Detection service. We protect customer estates 24x7x365. ZenSOC MDR services, powered by Microsoft Sentinel enables the collection of data and events from customer networks; it then analyses and correlates these events and reports on activity outside the normal that may indicate a potential security threat e.g. malware. Using our correlation rule set and our expert security analysts we separate the irrelevant from the suspicious or critical and then alert and respond the incident of any security issues and where applicable advice on remedial action.

3 Overview

Our ZenSOC platform is a subscription-based model that provided security monitoring, manage threat detection and response capabilities using best in class Tools & Technologies, Processes, People and Facilities to its customers. ZenSOC is fully prescriptive and provides a proactive yet adaptive way to hunt for the vulnerabilities and respond to them in a centralized, automated way by leveraging AI/ML-based technology; solving swivel chair problems and reducing dwell time. The salient features of Zen SOC services are below:

1. Fully co-managed services with Next-Gen SIEM
2. 24x7 monitoring across your entire IT ecosystem covering IoT, 5G, OT etc.
3. Detection, Investigation and Escalation of threats & incidents
4. Human-led threat hunting based on the mind-mapping exercise
5. Recommendation, Mitigation and Best Practices to improve the efficiency of security operations.
6. Compliance against key regulations and standards
7. Built continuity / resilience to make the business disruption proof.

3.1 Major Components in ZenSOC, powered by Microsoft Sentinel



- **Dashboards**: Customers will have access to real time network information – showing security incidents/offences by severity, location and category - in an accessible, easy to understand format. It will provide a number of pre-configured reports. It will empower the customer to take control of their network and take appropriate control action.
- **Rule**: A MDR or SIEM rule, is a logical expression that causes the system to take a specific action if a particular event occurs. For example, "If a user fails to log in correctly 3 or more times in 5 minutes generate an offence". When a SIEM Rule fires it automatically generates a case to alert a ZenSOC analyst to investigate and take appropriate actions.
- **Cases**: A case aggregates all the relevant evidence for a specific investigation. It can contain one or multiple alerts, which are based on the analytics that you define.
- **Hunting**: This is a powerful tool for investigators and security analysts who need to look for security threats proactively. The searching capability is powered by Kusto Query Language (KQL).
- **Notebooks**: By integrating with Jupyter Notebooks, Microsoft Sentinel extends the scope of what you can do with the collected data. The notebooks feature combines full programmability with a collection of libraries for machine learning, visualisation and data analysis
- **Data Connectors**: Built-in connectors are available to facilitate data ingestion from Microsoft and partner solutions.
- **Playbooks**: A Playbook is a collection of procedures that can be automatically executed upon an alert triggered by Microsoft Sentinel. Playbooks leverage Azure Logic Apps, which help you automate and orchestrate tasks/workflows. The purpose of a Cyber Security Playbook or Security Playbook is to provide all members of an organisation with a clear understanding of their roles and responsibilities regarding cyber security – before, during and after a security incident.
- **Analytics**: enable you to create custom alerts using Kusto Query Language (KQL).

- **Community**: The Microsoft Sentinel Community page is located on GitHub. It contains Detections based on different data sources that you can leverage to create alerts and respond to threats in your environment. The Microsoft Sentinel Community page also contains hunting query samples, playbooks and other artefacts.
- **Log Analytics workspace** is a container that includes data and configuration information. Microsoft Sentinel uses this container to store the data that you collect from the different data sources.
- **Reports**: A series of auto generated reports are provided with the ZenSOC platform that help customers manage the security of their network. These reports can be regularly reviewed with the customer by Zensar and appropriate guidance will be provided on how best to protect the customer's network.

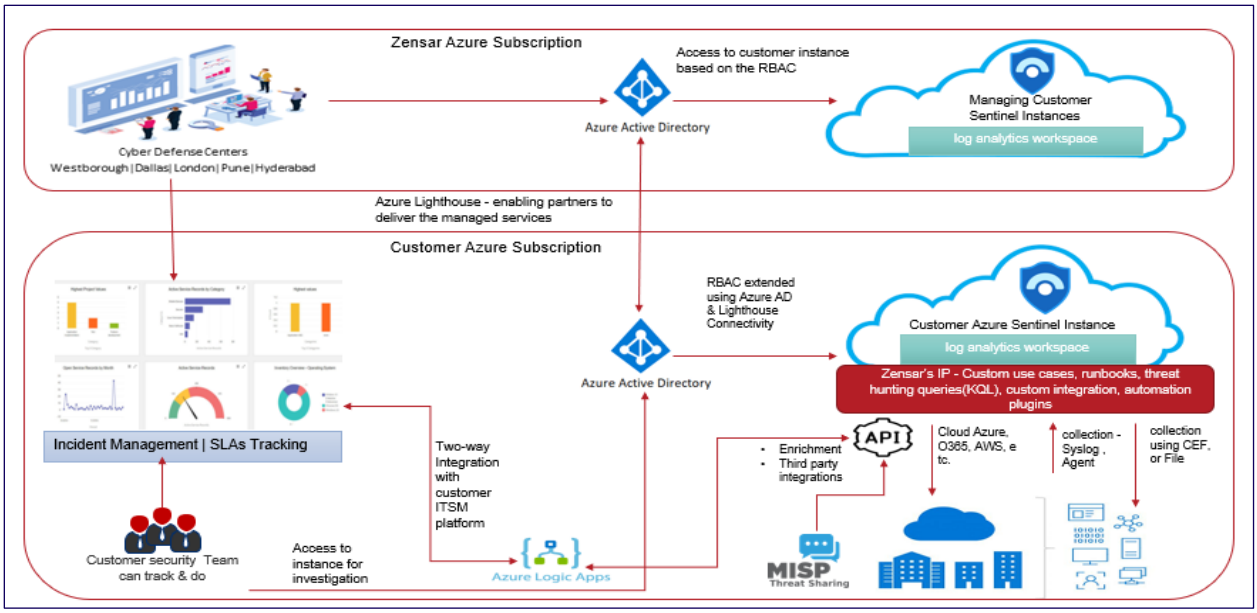
4 ZenSOC Potential Benefits

Our offering is flexible and deliver many potential benefits to clients. Some of them are highlighted as below:

- One-stop service to monitor all security device solution
- Extensive Threat Visibility
- Continual detection of attacks
- Reduction in False positive reporting
- Improvement in Mean time to Detect (MTTD) & Mean time to Respond (MTTR)
- Reduction in CAPEX & OPEX costing
- Measured Services based of KPI's and SLA's
- Fully certified experts
- Advanced security analytics
- Integrated Intelligence

5 High- Level Architecture

The diagram below shows the topology of the technical architecture. The overall architecture consists of multiple smaller components; Log Sources, event collection, dashboard, threat intelligence feeds and MISP platform intelligence.



6 ZenSOC Locations

Delivery Component	Description
Log Sources	• Customer Specific
MS Sentinel	• ZenSOC Powered by Microsoft Sentinel Or Customer Instance- anywhere
ZenSOC	Hyderabad, India (DC), Pune, India (DR)
Service Window	Security Incident Monitoring • 24x7x365 near real time security event monitoring and analysis
Certifications	ISO 27001-2013, HIPAA, GDPR Compliant

7 Connectivity

All Connectivity between customers to the MS Sentinel to the ZenSOC will be over an outbound TCP/443 connection via the internet.

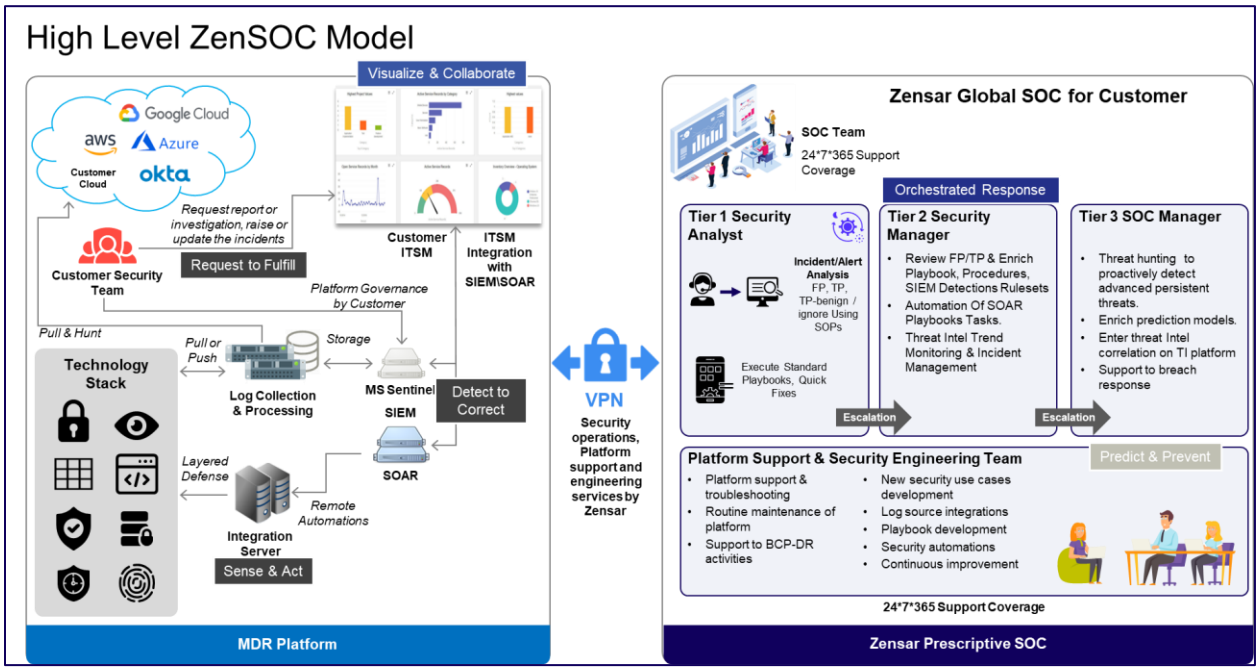
8 Security Tools

The table below provides a list of security tools being used in the ZenSOC platform.

Functionality	Tool
SIEM	Microsoft Sentinel
SOAR	Azure Logic Apps
Ticketing and Workflow	Service Now
Threat Intelligence	Commercial and open-source threat intelligence feeds
Visibility & Reporting	Microsoft Sentinel

9 Operational Model

This section describes the services teams employed in managing the ZenSOC delivery.



The following operational teams underpin and support the ZenSOC offering:

- Tier 1: Security Analysts
- Tier 2: Security Manager
- Tier 3: SOC Manager
- Platform Support & Security Engineering Team

- **Tier 1**: Security Analysts: They are cybersecurity first responders. Monitor security events displayed in the management consoles and process each event according to a well-defined Playbook. 1st Line response will raise and manage tickets, perform basic investigations to provide further context to reported incidents or discard false positives at an early stage and escalate potential true positives to Level 2 (within ZenSOC or the customers organisation) using playbooks.
- **Tier 2**: Security Manager: Responsible for supporting, monitoring and troubleshooting efforts as it relates to ZenSOC Operations working with SIEM technologies and other core network security products. Level 2 determine if a critical system or data set has been impacted and provide support for new analytic methods for detecting threats. Level 2 will escalate to Level 3 (within ZenSOC or the customers' organisation) as required for given incidents.
- **Tier 3**: SOC Manager: Take escalations from Level 2 Cyber Analysts and use the investigations carried out by previous teams to continue managing an incident effectively. 3rd Line also provide flexible specialist resources to commercial delivery teams to support commercial activities (incident response, technical consultancy services).They are involved in proactive threat hunting search through networks, endpoints and datasets to hunt malicious, suspicious or risky activities that have evaded detection by existing tools.

In addition to this, they will be responsible for the SOC team. They direct SOC operations and are responsible for syncing between analysts and engineers; hiring; training; and creating and executing on cybersecurity strategy.

Platform Support & Security Engineering Team: This team is comprised of the content development team, platform support and testing (DevOps team and Release Engineering/QA) team. They are responsible for infrastructure, application support and release cycle. The Cyber engineering team is responsible for all of the supporting infrastructure and systems underpinning the ZenSOC platform.The Content Development team is responsible for determining and developing the correct use cases for the customer environment as well as verifying the appropriate log sources are present and the supporting SIEM rules are in place. The role may or may not be customer facing depending on the presence of requirement. This is highly technical that are responsible for tuning rules in life, which is dependent on the service level that the customer takes. They focus on the nuts and bolts of security monitoring and use case development and implementation.

10 Service Tiers

To address customers' demand for a Managed Security Service across their network; we have developed a tiered service model that is technology agnostic and, consistent across our Security Portfolio. Because customers vary in terms of security risk, appetite and in-house capability; we have tiered this service to allow customers to take advantage of the service level most appropriate to their needs and capabilities.

We therefore offer three service tier options:

- Standard
- Enterprise
- Advanced

The service wrap around ZenSOC provides the various flavours covering different aspects of security services. Customer can select from the below services wrap and services will be delivered based on them.

Plan	Standard	Enterprise	Advanced
Continuous (24x7x365) security monitoring by SIEM solution	☑	☑	☑
Alerts Triage and validation eliminating false positive	☑	☑	☑
Raise incident tickets using client/ Zensar provided ITSM tools (**Incase of fully Shared Services, Zensar will use its own ticketing tool)	☑	☑	☑
Tracking & closure of security incidents	☑	☑	☑
Incident Investigation and Triaging	☑	☑	☑
Threat Intelligence feeds	☑	☑	☑
End Point detection and remediation(EDR)		☑	☑
End-to-End investigation & computer emergency & incident response (remote)			☑
Security Advisor related to Zero-day, Situation Awareness & Industry specific campaign		☑	☑
Manual Threat Hunting to find malicious or potentially harmful activity in client environment (Remote 8X5)		☑	☑
Automation & Response using SOAR capabilities			☑
Brand Monitoring Services			☑
VIP Credential monitoring			☑
Access to security intelligence portal			☑
Rule based correlation	☑	☑	☑
Compliance Reporting	☑	☑	☑
Monthly Threat hunt Report		☑	☑
State of the service reporting	☑	☑	☑
State of the service summary reporting	Quarterly	Monthly	Monthly

Service Coverage - 24 x7 Monday to Sunday – (Customer time zone / Delivery time zone).

Note: It will be depending upon which options selected by customer for their services during contract/SoW agreement.

11 Charging Units

ZenSOC charges are calculated based on the data ingested inside the SIEM solution and service wrap opted by client.

Sr.No.	Model	Charging Unit

1	Cloud Ingestion	Data ingested in GB
2	Service Wrap opted	Standard/ Enterprise/ Advanced

** Threat Hunting and SOAR related activities will be charged based on T&M basis.

12 Use Cases

ZenSOC has more than 400+ use cases based on the MITRE ATT@CK based framework. During the due-diligence phase, ZenSOC team will understand customer's requirements, business objectives and environment before enabling these use cases. Below are some use cases for Windows, Azure Active Directory, Palo Alto firewall, DNS, etc.

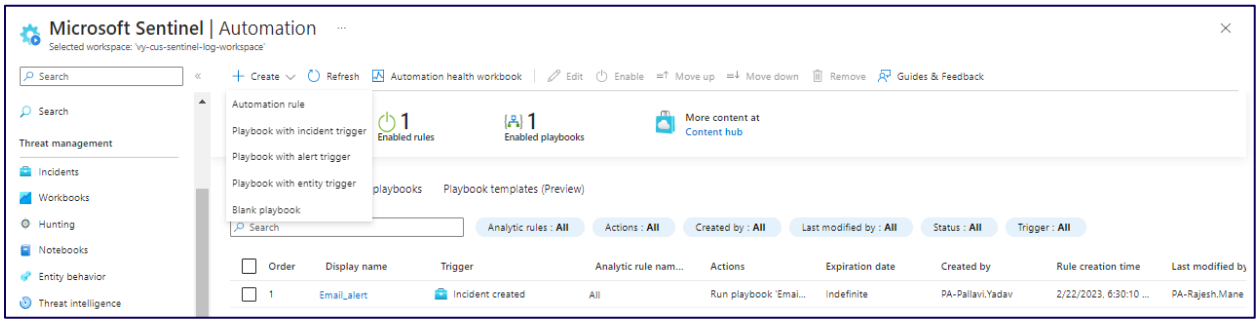
12.1 Custom Use Cases

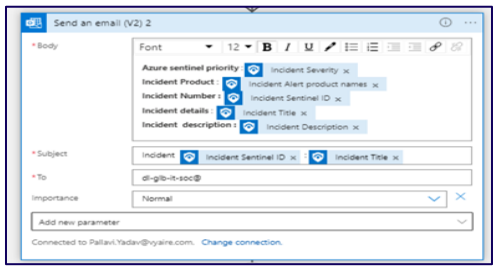
Zensar will create custom use cases if there is a unique requirement from the customer side. Below are some custom use cases examples.

1. Windows System health based on heartbeat.
2. Tracking Palo Alto firewalls based on last log received, if we don't receive the logs in defined period it will generate alert.
3. AWS Guard Duty based on last log received, if we don't receive the logs in defined period it will generate alert
4. AWS severity such as high. Example, AWSGuardDuty, where Severity between (7 .. 9)
5. AWS severity such as Medium. Example, AWSGuardDuty, where Severity between (4 .. 7)

12.2 Playbook

A playbook can help automate and orchestrate your threat response; it can be run manually on-demand on entities and alerts or set to run automatically in response to specific alerts or incidents when triggered by an automation rule. Following are snippets of the same:



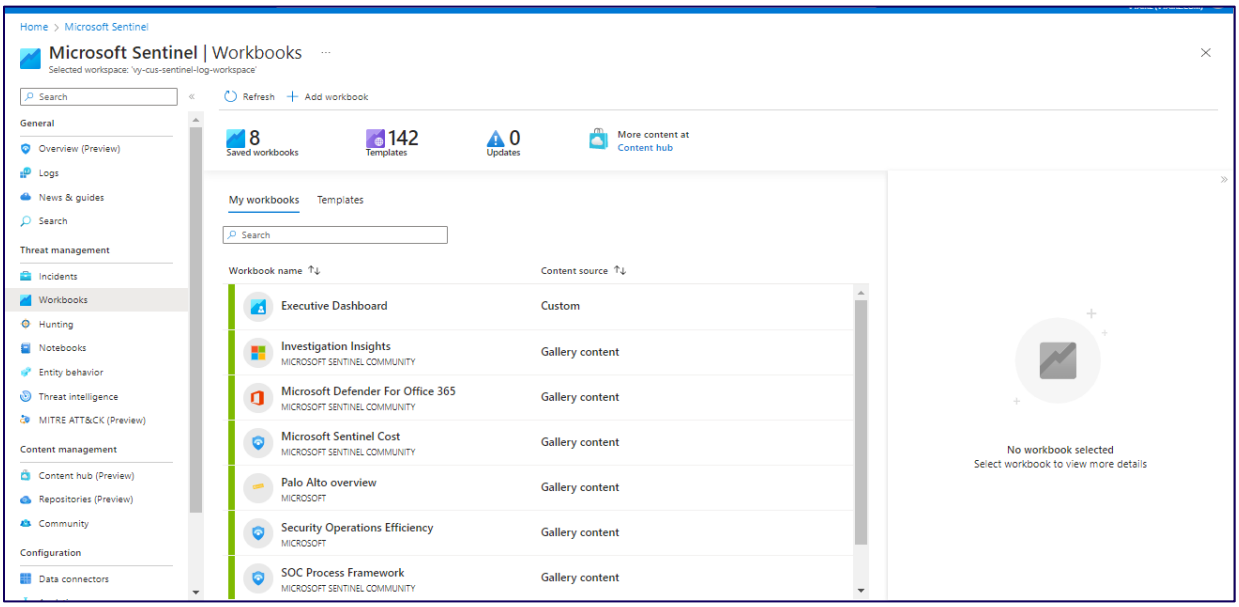


12.3 Workbook/ Dashboard

ZenSOC has more than 142 inbuild dashboards. However, we can discuss this with customer during the due-diligence phase.

Below are the out of box dashboard

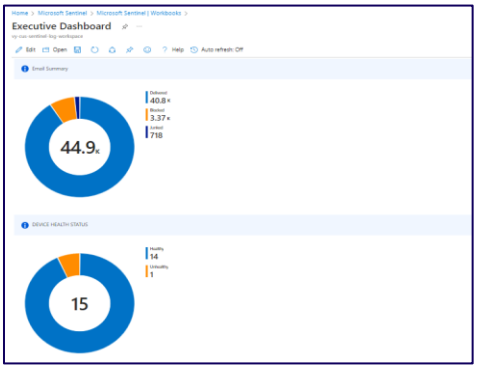
- Overview Dashboard
- Investigation Insights
- Palo Alto overview
- Security Operations Efficiency
- SOC Process Framework



12.4 Customized Dashboard

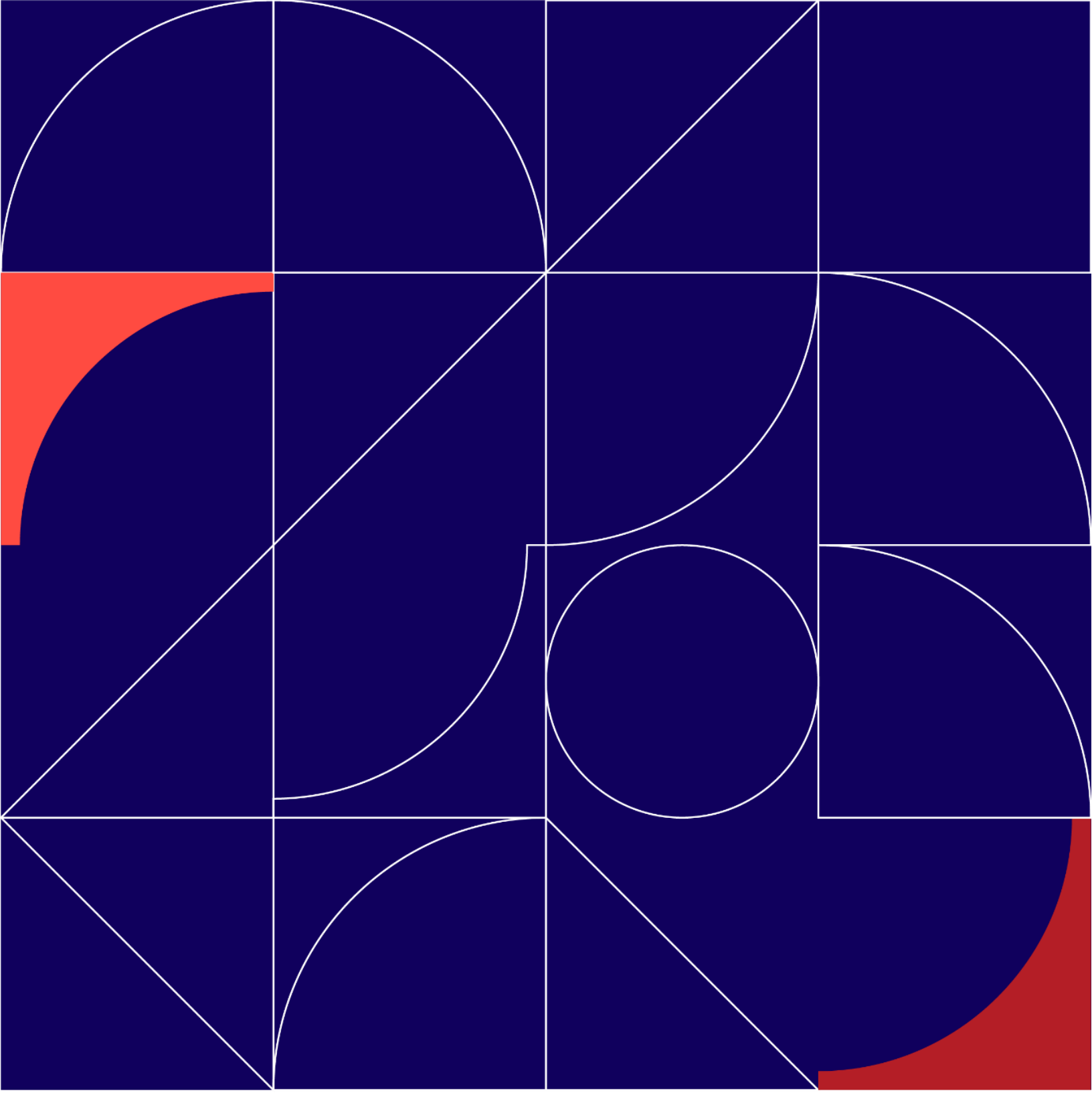
Zensar developed customized dashboard based on the customer requirement.

12.5 Executive Dashboard



13 Conditions in Contract/Agreement

- This Service Agreement will be applicable for customer's IT infrastructure on Production, UAT and Development environments.
- SLA wavier for initial period (3 Months) under stabilization period in case of new transition of services.
- Alerts Optimization will require at least 3 months.
- Customer provided ITSM tools will be in used and ownership will be with customer to manage and support tool platform.
- This Service Agreement will be reviewed annually.



We conceptualize, build and manage digital products through experience design, data engineering and advanced analytics for over 130 leading companies. Our solutions leverage industry-leading platforms to help our clients be competitive, agile and disruptive while moving with velocity through change and opportunity.

With headquarters in Pune, India, our 10,000+ associates work across 33 locations, including San Jose, Seattle, Princeton, Cape Town, London, Singapore and Mexico City.

For more information please contact: **marketing@zensar.com** | **www.zensar.com**

An RPG Company